Santa Clara High Technology Law Journal

Volume 21 | Issue 4 Article 1

2005

Virtual Speech: At the Constitutional Crossroads

Wendy Freedman

ARTICLES

VIRTUAL SPEECH: AT THE CONSTITUTIONAL CROSSROADS

Wendy Freedman†

Open source software has changed the landscape of IP litigation and altered the Internet-based marketplace for digital entertainment. Open source software is free, and no one controls its distribution rights. Thus, it has dramatically altered existing business relationships. The impact on intellectual property and entertainment litigation has been dramatic. In California, lawyers once confined to tangible property now must extend existing law to virtual reality—a minefield for the unwary practitioner.

OPEN SOURCE SOFTWARE

Proprietary commercial software vendors operate in an industry of highly protected trade secrets. "Open Source" is a term used by some to describe "free software."[1] Open source proponents believe that scientific knowledge must be shared and distributed.[2] Thus, the genesis of open source—the idea is that "source" code is fundamental to the furtherance of computer science and is freely available—is necessary for innovation to continue.

† Ms. Freedman is an attorney in Century City, California. Her practice consists of intellectual property and business litigation with an emphasis on First Amendment, entertainment and media law matters. She has a history of representing software development companies, cosmetic manufacturers and pharmaceutical companies in a variety of claims. She has represented entities in a variety of contract and licensing matters, including negotiating and drafting forms of computer-related agreements. Ms. Freedman serves as Secretary of the Beverly Hills Bar Association Barristers and received the Lawrence J. Blake Award as "Barrister of the Year" in September 2004.

1. *See* Richard Stallman, *Why Software Should Not Have Owners*, *at* http://www.gnu.org/philosophy/why-free.html (last visited Apr. 19, 2005); Open Source Initiative, *History of OSI*, *at* http://www.opensource.org/docs/history.html (last visited Apr. 19, 2005).

2. *See* Stallman, *supra* note 1; Open Source Initiative, *supra* note 1.

A series of guidelines have been crafted to describe software qualified as Open Source.[3] The Open Source Definition allows

3. *See* Bruce Perens, *The Open Source Definition, Version 1.0*, *available at* http://perens.com/Articles/OSD.html (last visited Mar. 13, 2005). The distribution terms of an open source program must comply with the following criteria:

> (1) Free Redistribution: The license may not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license may not require a royalty or other fee for such sale.
>
> . . .
>
> (2) Source Code: The program must include source code, and must allow distribution in source code as well as compiled form. Where some form of a product is not distributed with source code, there must be a well-publicized means of downloading the source code, without charge, via the Internet. The source code must be the preferred form in which a programmer would modify the program. Deliberately obfuscated source code is not allowed. Intermediate forms such as the output of a preprocessor or translator are not allowed.
>
> . . .
>
> (3) Derived Works: The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.
>
> . . .
>
> (4) Integrity of The Author's Source Code: The license may restrict source code from being distributed in modified form only if the license allows the distribution of "patch files" with the source code for the purpose of modifying the program at build time . . . . The license must explicitly permit distribution of software built from modified source code. The license may require derived works to carry a different name or version number from the original software.
>
> . . .
>
> (5) No Discrimination Against Persons or Groups: The license must not discriminate against any person or group of persons.
>
> . . .
>
> (6) No Discrimination Against Fields of Endeavor: The license must not restrict anyone from making use of the program in a specific field of endeavor.
>
> . . .
>
> (7) Distribution of License: The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.
>
> . . .
>
> (8) License Must Not Be Specific to a Product: The rights attached to the program must not depend on the program's being part of a particular software distribution. If the program is extracted from that distribution and used or distributed within the terms of the program's license, all parties to whom the program is redistributed should have the same rights as those that are granted in conjunction with the original software distribution.
>
> . . .
>
> (9) License Must Not Contaminate Other Software: The license must not place restrictions on other software that is distributed along with the licensed software.
>
> . . .

greater liberties with licensing. Therefore, the free redistribution of open source software by proprietary software vendors stands in contrast to current business practices, which thrive on the trade secrets, copyrights, patents and licenses that make distributing software profitable. The term "free software" does not describe its price but rather, the right to access the software's source code and includes the freedom to run, modify and redistribute copies or modified versions of the program.[4] Some companies, including major players in media-based industries, regard free, open source software as a serious threat to their intellectual property ("IP") and financial interests.

The paradigm shift between the free speech rights advocates and the companies co-opting source code for their own profitability is most pronounced in the most recent case, *DVD Copy Control Association v. Bunner*[5] ("*Bunner*"), that has resolved the convergence between California's trade secret law, section 3426 of the California Civil Code,[6] and the free speech clauses of the United States and California Constitutions.

TRADE SECRET ACTIONS

In order to obtain an injunction prohibiting disclosure of an alleged trade secret, a plaintiff's first hurdle is to show that the information it seeks to protect is indeed a trade secret.[7] California has adopted without significant change the Uniform Trade Secrets Act ("UTSA").[8] Combinations of general concepts are also protectable as trade secrets. A California Superior Court found that a computer program was entitled to trade secret recognition for the "specific implementation involving a particular combination of general concepts . . . even though all or some of them might well be known to the industry."[9]

---

(10) Example Licenses: The GNU GPL, BSD, X Consortium, and Artistic licenses are examples of licenses that we consider conformant to the Open Source Definition.

Id.

4. *Id.*

5. DVD Copy Control Ass'n, Inc. v. Bunner, 75 P.3d 1 (Cal. 2003).

6. Uniform Trade Secrets Act, CAL. CIV. CODE § 3426 (West 2005).

7. *Id.* § 3426.2.

8. *Id.* §§ 3426–3426.6; *see* Cadence Design Sys., Inc. v. Avant! Corp., 57 P.3d 647, 650 (Cal. 2002) (citations omitted).

9. Cybertek Computer Prods., Inc. v. Whitfield, 203 U.S.P.Q. (BNA) 1020, 1024 (Cal. Super. Ct. 1977).

Similarly, the U.S. District Court for the Northern District of California concluded that a computer program contained elements that entitled it to trade secret protection. The court noted that a trade secret could consist of the individual units of the computer program, its overall "architecture," structure or a combination thereof, as long as the program otherwise meets the value and secrecy requirements.[10] Software may constitute a trade secret.[11]

An action for the misappropriation of trade secrets is another vehicle that companies can use to protect their software. Trade secret misappropriation occurs whenever a person: (1) acquires another's trade secret with knowledge or reason to know "that the trade secret was acquired by improper means"[12]; (2) discloses or uses, without consent, another's trade secret that the person,

> [a]t the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was: (i) [d]erived from or through a person who had utilized improper means to acquire it; (ii) [a]cquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (c) [d]erived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use[13];

or (3) discloses or uses, without consent, another's trade secret that the person "[b]efore a material change of his or her position, knew or

---

10. Integral Sys., Inc. v. Peoplesoft, Inc., No. C-90-2598-DLJ, 1991 WL 498874, at *13, *16 (N.D. Cal. July 19, 1991).

11. Under California's version of the UTSA, trade secrets have been defined as

> information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

CAL. CIV. CODE § 3426.1(d); UNIF. TRADE SECRETS ACT § 1 (amended 1985), 14 U.L.A. 438 (1990); Duncan v. Stuetzle, 76 F.3d 1480, 1487 (9th Cir. 1996); *see also* Cybertek Computer Prods., Inc., 203 U.S.P.Q. at 1024–25; 1 ROGER M. MILGRIM, TRADE SECRETS § 1.08[5] (2004). Title III of the Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2886–87 (1998) (codified as amended at 17 U.S.C. § 117 (1998)) legislatively overrules the case of *MAI Systems Corporation v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), *cert. denied*, 510 U.S. 1033 (1994). Under 17 U.S.C. § 117, it is not "infringement for the owner or lessee of a machine to make or authorize the making of a copy of a computer program if such copy is made solely by virtue of the activation of a machine that lawfully contains an authorized copy of the computer program, for purposes only of maintenance or repair of the machine." 17 U.S.C. § 117(c) (2005). The section only applies if the new copy is used in no other manner and is destroyed immediately after the completion of the maintenance or repair, and if no computer program which is not necessary to the maintenance or repair is accessed. *See id.*

12. Uniform Trade Secrets Act, CAL. CIV. CODE § 3426.1(b)(1) (West 2005).

13. *Id.* § 3426.1(b)(2)(B).

had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake."[14]

Acquisition of a trade secret by "'[i]mproper means' includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[15] "Reverse engineering or independent derivation alone," however, is not "considered improper means."[16]

California's trade secret law provides a trade secret owner with several remedies against a misappropriator, including injunctive relief.[17] Indeed, section 3426.2, subdivision (a) expressly states that "[a]ctual or threatened misappropriation may be enjoined."[18] Thus, California law contemplates the use of injunctive relief as a remedy for trade secret misappropriation.[19]

TRADE SECRETS IN COMPUTER CODE

Although skilled in addressing trade secret claims, litigators may find that the case law is not clear when it comes to determining how to proceed when trying to enforce trade secrets in computer code. One option is to move for a preliminary injunction to prevent the further misappropriation of trade secrets. Case law illuminates that posting works online may interfere with the enforcement of trade secret rights, however.

Construing the elements of trade secret law in the context of the Internet, the court in *Religious Technology Center v. Netcom On-Line Communications Services, Inc.* defined the contours of the requirement that trade secrets not be "generally known."[20] Determining whether trade secret protection is lost for information on the Internet depends predominantly on the extent of the spread of the information. The court in *Religious Technology Center* raised this issue in a case brought against former members of the Church of Scientology for posting trade secrets online.[21] In that case, the court

14. *Id.* § 3426.1(b)(2)(C).

15. *Id.* § 3426.1(a).

16. *Id.* Reverse engineering is the process by which one starts with a known product and works backward to determine how it was developed or manufactured. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974).

17. *Id.* § 3426.2.

18. Uniform Trade Secrets Act, CAL. CIV. CODE § 3426.2(a) (West 2005).

19. DVD Copy Control Ass'n, Inc. v. Bunner, 75 P.3d 1 (Cal. 2003).

20. 923 F. Supp. 1231, 1256–57 (N.D. Cal. 1995); *see also* Religious Tech. Ctr. v. NetCom On-Line. Communication Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

21. *See generally Religious Tech. Ctr.*, 923 F. Supp. at 1250–57.

held that evidence demonstrating that others put material in the public domain prevented the plaintiff from enforcing its trade secret rights in the documents.[22] The court concluded that

> [w]hile the Internet has not reached the status where a temporary posting on a newsgroup is akin to publication in a major newspaper or on a television network, those with an interest in using the Church's trade secrets to compete with the Church are likely to look to the [alt.religion.scientology] newsgroup [where the documents were posted]. Thus, posting works to the Internet makes them "generally known" to the relevant people . . . .[23]

FIRST AMENDMENT AND ANTI-CIRCUMVENTION CASES

After legislation such as the Digital Millennium Copyright Act was enacted,[24] several cases arose interpreting whether technology that circumvents protection systems facilitates copyright infringement. In particular, these cases examined the convergence between copyright law and the First Amendment—a foreshadowing of the *Bunner* decision.[25] In the precursor case, *Universal City*

---

22. *Id.* at 1256.

23. *Id.*

24. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998). The DMCA was enacted as an amalgamation of five titles: (1) implement the WIPO Internet Treaties; (2) establish safe harbors for online service providers; (3) permit temporary copies of programs during the performance of computer maintenance; (4) make miscellaneous amendments to the Copyright Act, such as amendments to the Copyright Act, including amendments which facilitate Internet broadcasting; and (5) create *sui generis* protection for boat hull designs. Since the promulgation of the DMCA, the Copyright Office conducted a rulemaking proceeding per the DMCA to determine whether there were any classes of works that should be exempt from the anti-circumvention provisions that took effect on October 1, 2000. The Office rejected numerous requests for broad exemptions (e.g. "all DVDs") and crafted two exemptions. The two exempted classes of works are: 1) compilations consisting of lists of websites blocked by filtering software applications and 2) literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access due to malfunction, damage or obsoleteness. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64582 (Oct. 27. 2000) (to be codified at 37 C.F.R. pt. 201).

25. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 307 (S.D.N.Y. 2000); *see* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 436 (2d Cir. 2001); *see also* RealNetworks, Inc. v. Streambox, Inc., No. 2:99CV02070, 2000 WL 127311 (W.D. Wash. Jan. 18, 2000). In *RealNetworks*, the court found that RealNetworks had demonstrated the likelihood of success on the merits of its claims that the Streambox VCR is a device that violates the anti-circumvention provisions of the DMCA. The court noted that StreamBox was primarily designed to circumvent technological measures that effectively control access to copyrighted works. The Streambox VCR caused the RealServer to recognize it was an authorized RealPlayer, and therefore allowed unauthorized copying of the streamed signal. The court agreed with RealNetworks that it is important for copyright owners to know that they can rely on content contained in streamed signals not being copied without their permission. *See* A&M

Studios, Inc. v. Reimerdes, the court granted the request of eight motion picture studios for an order barring defendants under section 1201(a)(2) of the DMCA from distributing a software program ("DeCSS") that decrypted digital versatile disks ("DVDs") encrypted using a software program called Content Scramble System ("CSS").[26] The court rejected the arguments that linking to DeCSS was a valid exercise of "free speech" rights under the First Amendment and the doctrine of "fair use" permits DeCSS.[27]

As such, "[i]t cannot seriously be argued that any form of computer code may be regulated without reference to First Amendment doctrine."[28] Of course,

> [n]ot everyone can understand each of these forms. Only English speakers will understand English formulations. Principally those familiar with the particular programming language will understand the source code expression. And only a relatively small number of skilled programmers and computer scientists will understand the machine readable object code. But each form expresses the same idea, albeit in different ways.[29]

Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001), *aff'd*, 284 F.3d 1091 (9th Cir. 2002) (upholding the district court's rulings that Napster was liable for contributory and vicarious infringement of record company and music publisher copyrights and held that "file sharing" constitutes an infringement of copyright). *See* Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1527–28 (9th Cir. 1992) (laying the groundwork for the legal analysis of copyright law and reverse engineering of software in announcing the following rule: "[W]here disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law."). *See also* Sony Computer Entm't, Inc., v. Connectix Corp., 203 F.3d 596, 609–10 (9th Cir. 2000) (reversing the district court's grant of a preliminary injunction on grounds of fair use, ruling that the creation of intermediate copies of firmware for the purpose of reverse engineering is fair use); UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349, 350 (S.D.N.Y. 2000) (granting summary judgment in favor of recording industry based on defendant's creation of online MP3 library through the unauthorized copying of commercial CDs into MP3 format; court rejected defendant's contention that service was "functional equivalent" of storing its subscribers' CDs, stating that "in actuality defendant is re-playing for the subscribers converted versions of the recordings it copied" and ruled infringement for the unauthorized copying of server copies of thousands of CDs by MP3.com for "My.MP3.com" service). The issues raised in the above cases are outside the scope of this paper, which seeks to explore the convergence of software reverse engineering and trade secret law, but they set the stage for the development of the law in the arena of intellectual property rights.

26. *Universal Studios, Inc.*, 111 F. Supp. 2d at 303.

27. *Id.* at 324, 341.

28. *Id.* at 326.

29. *Id.* at 326.

The California court is not alone in concluding that computer code, and computer programs constructed from code can merit First Amendment protection.[30]

CONSTITUTIONALITY OF INJUNCTION

First Amendment jurisprudence must be examined when determining the constitutionality of an injunction prohibiting the dissemination of computer code.[31] In determining the appropriate level of scrutiny, the critical question is whether the injunction is content-neutral or content-based.[32] Content-based injunctions are subject to the level of heightened scrutiny set forth in *Perry Education Assication. v. Perry Local Educators' Association.*[33] Content-neutral injunctions are subject to the lesser level of scrutiny set forth in *Madsen v. Women's Health Center.*[34]

One principal inquiry in determining content-neutrality is "whether the government has adopted a regulation of speech 'without reference to the content of the regulated speech.'"[35] "The government's purpose is the controlling consideration," and a governmental regulation of speech is content-based if the government adopted the regulation "because of disagreement with the message it conveys."[36] Thus, an injunction "that serves purposes unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some speakers or messages but not others."[37]

CONVERGENCE OF FIRST AMENDMENT LAW AND TRADE SECRET LAW

Although other cases have raised the issue of the applicability of the Digital Millennium Copyright Act ("DMCA") to claims of copyright infringement in the context of the First Amendment, until the *Bunner* decision, no California court had analyzed whether enjoining the downloading of online music and/or digital content that is accorded trade secret protection violates First Amendment law.

---

30. *Id.* at 327; Junger v. Daley, 209 F.3d 481, 484 (6th Cir. 2000); United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1126–27 (N.D. Cal. 2002).

31. *Reimerdes*, 111 F.Supp.2d at 327.

32. *See* Madsen v. Women's Health Ctr., Inc., 512 U.S. 752, 762–64 (1994); Los Angeles Alliance for Survival v. Los Angeles, 993 P.2d 334, 340-41 (Cal. 2000).

33. 460 U.S. 37, 45 (1983).

34. *Madsen*, 512 U.S. at 765.

35. *Id.* at 763 (quoting Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989)).

36. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

37. *Id.* at 791.

For example, in *Bunner*, the DVD Copy Control Association filed and preliminarily won in an action in the Supreme Court of California against Andrew Bunner, one of two dozen individuals who posted a program called DeCSS, which enabled individuals to play DVD movie files on their PCs as they would any regular multimedia file.[38] The programmers used reverse engineering to figure out how to unlock the DVD encryption system.[39] Proponents of free software want to be able to display the films on Linux computers, while the DVD industry and movie studios fear the impact that such software will have on protecting their intellectual property.

Digital versatile discs (DVD's) "are five-inch wide disks capable of storing more than 4.7 [Gigabytes] of data" and "are used to hold full-length motion pictures in digital form."[40] To prevent piracy, the motion picture, computer, and consumer electronics industries used an encryption scheme known as the Content Scrambling System ("CSS") to encrypt copyrighted content on DVDs.[41] To this end, they began licensing the technology in October 1996 and formed the DVD Copy Control Association, Inc. ("DVD CCA") as the entity charged with granting and administering the licenses to the CSS technology.[42] Jon Johanson acquired the proprietary information and wrote a program called DeCSS that decrypts movies stored on DVDs and enables users to copy and distribute these movies.[43] Bunner posted DeCSS on his Web site because "it would enable 'Linux' users to use and enjoy 'DVDs' available for purchase or rental in video stores" and "make 'Linux' more attractive and viable to consumers."[44] "Bunner also claimed he wanted 'to ensure [that] programmers would have access to the information needed to add new features, fix existing defects and, in general, improve the '[D]eCSS' program.'"[45]

In the complaint, DVD CCA did not seek damages, but rather sought an injunction.[46] In issuing a temporary restraining order, the court concluded that DVD CCA was likely to prevail on the merits

38. DVD Copy Control Ass'n, Inc. v. Bunner, 75 P.3d 1, 6–7 (Cal. 2003).

39. *Id.* at 7.

40. *Id.* at 6 (quoting Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 307 (S.D.N.Y. 2000) (footnote omitted)).

41. *Id.* at 6–7.

42. *Id.* at 7.

43. *Id.*

44. *Bunner*, 75 P.3d at 7.

45. *Id.*

46. *Id.* at 8.

and would suffer irreparable harm without injunctive relief.[47] The Court of Appeal reversed, holding that the preliminary injunction, even if justified under California's trade secret law, violated the First Amendment.[48] The Supreme Court resolved the narrow question, whether the preliminary injunction violates Bunner's right to free speech under the United States and California Constitutions, even though recognizing the DVD CCA is likely to prevail on its trade secret claim against Bunner.[49]

The court determined that the restrictions on the dissemination of computer code in the form of DeCSS are subject to scrutiny under the First Amendment.[50] But the Supreme Court held that the preliminary injunction issued by the trial court burdened no more speech than necessary to serve the significant government interest promoted by California's trade secret law.[51] The court found that the preliminary injunction issued by the trial court was content-neutral since the underlying basis for the injunction was the trial court's holding that Bunner misappropriated DVD CCA's trade secrets in violation of California's trade secret law.[52]

The *Bunner* court found that First Amendment interests served by the disclosure of purely private information like trade secrets are not as significant as the interests served by the disclosure of information concerning a matter of public importance.[53] Because the injunction was determined to be content-neutral and was issued because of Bunner's prior unlawful conduct, the Supreme Court concluded it was not a prior restraint and therefore did not violate the First Amendment.[54]

As the *Bunner* court recognized, trade secret law recognizes the value of technologies and the brief window of opportunity to maximize the marketing and sale of these technologies.[55] To capitalize on private investment, companies must prevent the secret information technology from being released to the public domain.

---

47. *Id.*

48. *Id.* at 8–9.

49. *See id.* at 9.

50. *Bunner*, 75 P.3d at 10.

51. *Id.* at 13.

52. *Id.* at 11.

53. *See id.* at 15 (citing Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 759 (1985) ("[S]peech on matters of purely private concern is of less First Amendment concern" than "speech on public issues.")).

54. *Id.* at 17.

55. *See Bunner*, 75 P.3d at 13 (citations omitted).

Oftentimes, this is effectuated through entering into confidential relationships with vendors, distributors and the like. The loss of a trade secret's status as secret jeopardizes the potential return generated by the original investment. For example, music companies recently have been forced to advance release dates when trade secrets are disseminated on the Internet, oftentimes incurring additional costs not only in monetary investment but also in squandered human capital.

Trade secrets also do not have the benefits of those afforded under the patent laws.[56] For example, provided an inventor discloses details about his or her invention to the public, he or she is entitled to an exclusive right to make, use and sell his or her invention. Nonetheless, a company's protecting an invention as a trade secret does not ensure the period of exclusivity enjoyed by patent-holders. Accordingly, laws to prevent anti-circumvention measures are necessary to defeat those who seek to take advantage of confidential disclosure via unlawful means—those who wittingly destroy trade secret status to unfairly compete in the marketplace.

Thus, the *Bunner* court premised its decision on the assumption that innovation is contingent on trade secret protection.[57] If companies could free ride on the development of new technologies, intangible property rights would cease to be exploited. And, research and development would be shortchanged as companies seek to capitalize on their market share, only to have individuals stealthily use, distribute or sell the very same trade secrets. By doing so, the protection afforded by trade secret law is effectively destroyed. Contrast this to the open source advocates who believe that innovation is actually fostered by freely available source or object code because modifications may increase the utility of products and maximize the inherent value of the intellectual property to consumers.

In sum, the Supreme Court reversed the Court of Appeal and remanded the case with instructions for the Court of Appeal to determine whether the evidence in the record supports the factual findings necessary to establish that the preliminary injunction was warranted.[58] On remand, the Court of Appeal held that the DVD Copy Control Association was required to show irreparable harm before obtaining an injunction, did not show a likelihood of prevailing

56. *See id.* (citing Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481,493 (1974)).

57. *Id.* at 13.

58. *Id.* at 19–20.

on the merits, and failed to show irreparable harm if the injunction were not issued.[59]

The court highlighted the inherent weakness of the case—the widespread dissemination of DeCSS and its trade secrets across the vast expanse of the Internet.[60] The secrecy of the alleged trade secrets had been dispersed across optical waves, across time zones, and across jurisdictions. The impetus for the DVD CAA to pursue its claims against Bunner was destroyed by the click of a mouse prior to Bunner ever posting DeCSS on his site. In fact, the court could not ascertain at what point in time Bunner actually posted the program.[61] Accordingly, there was insufficient evidence produced to establish that the information contained in DeCSS was still secret.[62] The failure to establish secrecy negated the element of irreparable harm—a requisite element of the misappropriation claim.[63] When it comes to the distribution of information claimed to be a trade secret, misappropriators benefit from reproducing trade secrets on a massive scale. Third parties could exploit such an opportunity to reap great benefits therefrom.

The court stated that DVD CCA had not shown a likelihood that it would prevail on the merits of its claim of misappropriation of trade secrets because the trial court did not make an express finding that the proprietary information contained in DeCSS was not generally known at the time Bunner posted it.[64]

EFFECTS OF FREE SOFTWARE AFTER *BUNNER*

Preliminary injunctions are worthwhile and do not violate the free speech clauses of the United States and California Constitution after *DVD Copy Control Association, Inc. v. Bunner*.[65] Although the decision was quite limited in holding that the preliminary injunction against the individuals who posted the free software on their website did not violate the free speech clauses of the United States and California Constitutions, the far-reaching effect of this decision is already influencing legislative developments and impacting the

59. DVD Copy Control Ass'n, Inc. v. Bunner, 10 Cal. Rptr. 3d 185, 196 (Cal. Ct. App. 2004).

60. *See id.* at 194.

61. *Id.*

62. *Id.* at 194–96.

63. *Id.*

64. *Id.* at 193.

65. DVD Copy Control Ass'n, Inc. v. Bunner, 75 P.3d 1, 6 (Cal. 2003).

Recording Industry Association of America's ("RIAA") strategy which has typically focused on filing copyright infringement suits against digital music portals and companies.[66]

Immediately after the Supreme Court's decision came down on August 25, 2003, the music industry filed lawsuits against individuals for the unauthorized digital delivery of thousands of songs to other people on file-sharing services like KaZaa and Morpheus.[67] The RIAA had previously been unsuccessful in pursuing similar relief against companies who created the devices under which MP3 files could be played.[68]

Nonetheless, the jury is still out in *Bunner*. On remand, the Court of Appeal, in finding that the preliminary injunction was not warranted, suggested that the widespread dissemination of the trade secret DeCSS, had in effect destroyed trade secret rights, leaving practitioners and anxious movie executives to await a final adjudication on the merits.[69] Most notably, the Court of Appeal recognized the analytical difficulties with this case, since it does not fit neatly into classic business or commercial law concepts.[70]

Developments in technology and consumer demand for the distribution of technologies via the Internet has altered the law in this area. Individuals and companies have created a network that uses the internet to connect people throughout the world, enabling individuals to pool various types of infringing digital files, including files containing motion pictures, music and other content. Unfortunately, the courts claim to have difficulty protecting intellectual property rights in this new terrain.[71]

Open source software has changed the landscape of IP litigation and altered the Internet-based marketplace. Historically, vendors of proprietary commercial software co-opted source code for

66. *See, e.g.*, UMG Recordings Inc. v. MP3.com, Inc., 56 U.S.P.Q.2d (BNA) 1376 (S.D.N.Y. 2000).

67. Amy Harmon, *261 Lawsuits Filed on Music Sharing*, N.Y. TIMES, Sept. 9, 2003, at A1; *see also* Neil Strauss, *Executives Can See Problems Beyond File Sharing*, N.Y. TIMES, Sept. 9, 2003, at C1.

68. *See* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys. Inc., 180 F.3d 1072 (9th Cir. 1999).

69. *See* DVD Copy Control Ass'n, Inc. v. Bunner, 10 Cal. Rptr. 3d 185, 194–95 (Cal. Ct. App. 2004).

70. *Id.* at 195.

71. Stay tuned as the U.S. Supreme Court hears arguments in the *MGM v. Grokster* case. A highly anticipated ruling is expected on whether companies that distribute peer-to-peer software are liable for the consumers' downloading of music and movies on the Internet.

profitability; the open source movement promotes the idea that freely available source code advances innovation.

In sum, not all companies have embraced the open source phenomenon, and open source threatens to erode a software company's IP. The recent upward trend in digitization has allowed the distribution of perfect copies of both movie and multimedia works, which poses a threat to traditional IP protection and an increased risk of piracy. Companies will seek to obtain and enforce their trade secrets and copyrights over protocols that will not be available to open source software.

Ultimately, lawmakers must strike a balance between protecting the IP rights of companies and promoting the free exchange of ideas. Recently, the Federal Communications Commission approved the first digital anti-piracy measure to require by 2005 that some personal computers and other consumer electronic devices be equipped with technology to help block Internet piracy of digital entertainment.[72] Recognizing that digital entertainment is more susceptible than encrypted cable or satellite programming to being captured and retransmitted via the Internet, the industry could embed a piece of digital code known as a "broadcast flag" under the new rules.[73]

As applied to new media, the anonymity preserved on the Internet encourages the free flow of information without regard to the source of such speech. Even with the advent of open source software, however, laws restricting the Internet do not have as their central tenet preserving speech through recognition of the source. Instead, the restrictions on the Internet focus on the receiver or listener's right to receive and use information. The IP model as applied to the Internet is imperfect in that it grants a patentee or copyright owner a property right in his or her work, but does not necessarily grant a correlating right for another user to gain access to the work or contribute further ideas or protect the users' right to privacy when viewing copyrighted materials. Hence, there is a conflict with free software advocates. Moreover, in light of *Bunner*, "[t]he anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation."[74]

---

72. *See* In the Matter of Digital Broadcast Content Protection, 18 F.C.C.R. 23,550 (Nov. 4, 2003).

73. *See id.*

74. *DVD Copy Control Ass'n, Inc.*, 10 Cal. Rptr. 3d at 195 (citing Religious Tech. Ctr. v. Netcom On-Line Communications Servs., Inc., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995).

It is the role of Congress to ensure that legal rules allocating rights to individuals do not violate the system of free expression or stifle innovation by permitting companies to use the existing IP model to monopolize code, which is the foundation for further technological development. And, it will be up to the judiciary to define the contours of the law in this area to promote access, integration and use of new mediums from which to view entertainment. Practitioners will likely look for continued negotiations between copyright owners and users for licensing, blanket licensing, and international cooperation regarding encryption rights to avoid the uncertain fate in the virtual reality at the constitutional crossroads.

***